Fortaleciendo el futuro

Resultados del IBM Chief Information Security Officer Assessment 2014



IBM Center for Applied Insights
ibm.com/ibmcai | **ibmcai.com**

Dicen que el futuro no tiene límites. Para los líderes en seguridad de la información, esta idea puede asustar. Responsables ya de proteger las empresas de una multitud de amenazas en constante cambio, ahora deben prepararse no solo para nuevas oleadas de ataques, sino también para atacantes más sofisticados.

Nuestro estudio señala lo que preocupa a los líderes de la seguridad actuales y lo que pueden hacer para gestionar las incertidumbres que se acercan.

En el mundo de las TI, el papel de vigía es cada vez más difícil. La innovación en la informática avanza a gran velocidad, generando nuevas tecnologías que, aunque impresionantes e impactantes, con frecuencia amplían las responsabilidades defensivas de los líderes de la seguridad. Además del entusiasmo que rodea la aparición de la movilidad, el cloud y Big Data, debe darse una importancia equivalente a la seguridad. Sin mencionar los retos existentes, tales como la gestión del riesgo TI, lidiar con las regulaciones y normativas, así como una colaboración eficaz.

El éxito no está ni mucho menos asegurado: ¿cuántas veces solo en este año las noticias hablan de infracciones de datos o problemas en la seguridad de la información? Aún cuando los directores de seguridad de la información (CISOs) intentan clarificar diversas amenazas en sus empresas, ellos mismos están bajo un foco intenso.

El CISO Assessment 2012 del IBM Center for Applied Insights, el primero de esta serie, definió tres tipos de líderes en la seguridad: el Reactivo, el Protector y el Influenciador, y empezó a explorar sus características. Un año más tarde, el CISO Assessment 2013 ofreció pasos prácticos para ayudar a que los líderes de la seguridad alcanzaran la posición de Influenciador y mostró cómo dicha transición podría definir un nuevo estándar en el liderazgo de la seguridad.

Acerca del estudio

Para conocer las condiciones actuales de los líderes de seguridad y sus opiniones sobre el futuro, el IBM Center for Applied Insights, en colaboración con IBM Security, llevó a cabo entrevistas en profundidad con 138 líderes de seguridad, los más altos ejecutivos de TI y de línea de negocio responsables de la seguridad de la información en sus organizaciones. Algunos de estos líderes tenían el cargo de CISO, pero dada la diversidad de estructuras organizativas, otros no. Entre los demás encuestados se encontraban directores de tecnologías de la información (CIO), vicepresidentes de seguridad TI y directores de seguridad. El 63% de organizaciones entrevistadas contaban con un CISO. La participación cubrió un amplio conjunto de sectores y 5 países distintos.

La edición del CISO Assessment correspondiente al año 2014 evalúa el estado actual de los líderes en seguridad y lo que esperan encontrarse en los próximos 3 a 5 años. Los líderes de la seguridad se encuentran en plena evolución. Impulsados por el espectro de los ataques externos y las necesidades de sus propias organizaciones, siguen en pleno progreso hacia una función de liderazgo de negocio centrado en la gestión del riesgo y la adopción de un enfoque más integrado y sistemático.

¿Cuál es la siguiente etapa en la evolución del líder de seguridad? Con sus vidas ya tan atareadas, ¿qué pueden hacer los líderes de seguridad para reforzar su preparación y mejorar sus previsiones?

Temas clave

1. Destacar en un entorno en continua transformación
2. Gran preocupación por las amenazas externas
3. Esperar más colaboración externa
4. Centrándose todavía en la tecnología actual
5. Incertidumbre en la acción gubernamental

Destacar en un entorno en continua transformación

Los líderes de la seguridad y sus organizaciones contemplan cambios radicales en el entorno que los rodea: el 82% de encuestados afirmaron que la propia definición de seguridad había cambiado en los últimos tres años. Las empresas ya no se limitan a pulir los detalles de sus políticas de seguridad; están reconsiderando estrategias enteras para tener en cuenta la expansión de datos, dispositivos, necesidades de los usuarios y la importancia global de la seguridad en cada rincón de la empresa.

Esta transformación va acompañada del correspondiente crecimiento de la función del CISO y similares. Mientras que en los años anteriores, muchos profesionales de la seguridad aspiraban a ser influenciadores estratégicos, el 61% de los encuestados de este año se consideran como tales. Además, el 64% valoraron la estrategia de seguridad documentada a nivel de empresa como muy madura. Este cambio es la evidencia de la madurez que está alcanzando la función de los líderes de seguridad en sus organizaciones cada vez más concienciadas.

Esta mayor autoridad no se basa en una necesidad especulativa. Los líderes de seguridad deberán utilizar su influencia para gestionar un conjunto más amplio de amenazas externas y mayores expectativas en la empresa. Un alcance más amplio de lo que necesita protección (por ejemplo, cloud, móviles, etc.) y las nuevas tecnologías en seguridad también aportan su grano de arena en esta tendencia a una mayor complejidad. Los CISOs ya no son representantes de la tecnología de seguridad, sino más bien tomadores de decisiones que siempre deben tener en cuenta las operaciones de negocio. Los líderes de la seguridad tienen más peso y lo ejercen para contribuir a los objetivos más amplios de las empresas, mientras gestionan el riesgo en cada uno de los pasos que se dan.

Obtener más influencia y soporte

Influencia

90% Muy de acuerdo en que tienen una influencia significativa en sus organizaciones

76% Dicen que su grado de influencia ha aumentado significativamente en los últimos tres años

Soporte organizativo

71% Muy de acuerdo en que reciben el soporte organizativo que necesitan

Colaboración interna

82% Participan en reuniones estratégicas o ejecutivas trimestralmente o con más frecuencia

62% Desarrollan su estrategia de seguridad conjuntamente con otras estrategias (principalmente TI, riesgo y operaciones)

Figura 1. Esta creciente madurez e influencia es necesaria para dar respuesta al entorno de amenazas externas más problemático.

Perspectiva del CISO: Un perfil más alto para retos más difíciles

CISO Jonathan Klein,
Broadridge Financial Solutions

Mi perfil como CISO ha aumentado en los últimos años. Ejerzo mayor influencia y me reúno regularmente con miembros de la Dirección y otros altos ejecutivos. Pero debido a que la seguridad de la información es cada vez más compleja, existen todavía muchos retos, por lo que mis responsabilidades y capacidades globales deben adaptarse a este ritmo. Broadridge presta una serie de servicios tecnológicos y de procesamiento para entidades financieras. En esta función gestionamos uno de los activos más valiosos de nuestros clientes: la información de los clientes.

Uno de los mayores retos a los que se enfrentan actualmente las empresas es la integración de la tecnología de la seguridad en los correspondientes procesos de negocio. Con frecuencia, las nuevas tecnologías prometen resolver la amenaza más reciente de seguridad, pero son ineficaces si no se integran correctamente en los procesos de negocio. Interactúo con los ejecutivos de Broadridge para integrar las consideraciones sobre la seguridad y el riesgo en las primeras etapas de sus decisiones de negocio y me aseguro de que la tecnología de seguridad no solo proteja a nuestra organización, sino que también evolucione con nuestros procesos y políticas de negocio.

Por ejemplo, existen varios estándares de datos que se supone que son herméticos. Muchas veces, las empresas esperan que la conformidad con estos estándares les garantice que la información sensible estará segura durante todo el ciclo de vida de los datos sin medidas complementarias. Esto ha demostrado ser una asunción peligrosa, como han puesto de manifiesto muchas infracciones de datos de perfil alto. En Broadridge, nos centramos en proteger los datos que procesamos y no solo marcar una casilla en un estándar de cumplimiento normativo.

La consumerización de las TI también crea complicaciones. Ya no existe una clara distinción entre el uso personal y profesional de dispositivos y aplicaciones. Esto lleva muchas veces al acceso público de tecnologías originalmente diseñadas para ser privadas. También hace que la seguridad vaya por detrás de las nuevas tecnologías que los consumidores adoptan rápidamente. Se pone más énfasis en las nuevas funciones que en la seguridad, lo cual dificulta a las empresas la adopción de dichas nuevas tecnologías de forma rápida, al mismo tiempo que evalúan todas sus implicaciones en la seguridad.

Asegurarse de que la seguridad es una piedra angular y no un toque final será un imperativo clave de la creciente influencia de la función del CISO.

Gran preocupación por las amenazas externas

Una mayor madurez e influencia es esencial ante el desafío planteado por las amenazas persistentes avanzadas, empresas criminales, piratas informáticos patrocinados por estados, “hacktivistas” y otros criminales cibernéticos. Tanto los líderes de seguridad como sus organizaciones consideran que esta amenaza es *tan* grande que muchos tienen la sensación de estar perdiendo la batalla. Cerca del 60% de líderes de seguridad entrevistados dijeron que la sofisticación de los atacantes superaba la sofisticación de las defensas de sus organizaciones. Más del 80% de líderes de seguridad han visto aumentar la amenaza externa en los últimos tres años y consideran que es el máximo desafío actual. Es más, el foco en las amenazas externas no disminuirá en el futuro, ya que la mitad de los líderes entrevistados afirmaron que se necesitará el máximo esfuerzo de la organización para resolverlo en los próximos tres a cinco años.

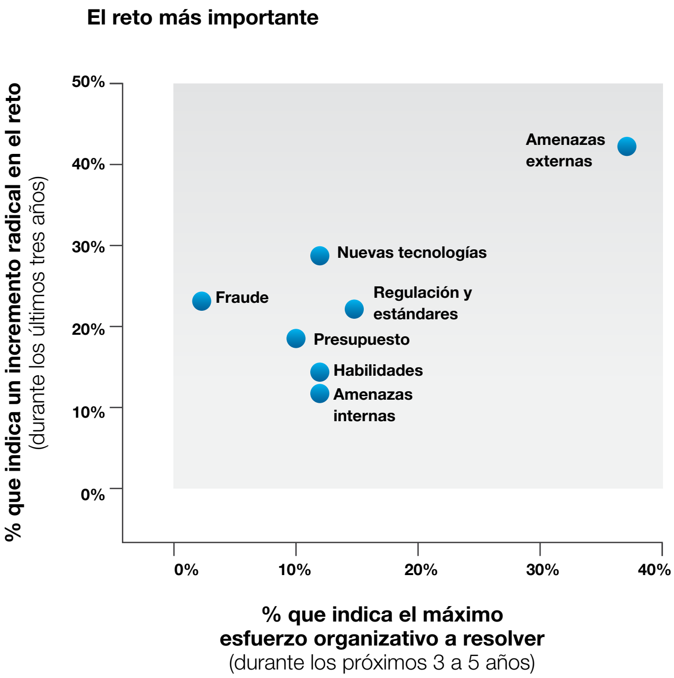


Figura 2. Los líderes de seguridad seguirán centrándose en las amenazas externas en el futuro inmediato, dedicados a disminuir el riesgo.

Perspectiva del CISO: Mejorar las estrategias de la seguridad mediante la colaboración

John Taylor
Antiguo Director Global de Seguridad TI, British American Tobacco

La colaboración externa ofrece a los líderes de seguridad la oportunidad de observar prácticas sectoriales y evolucionar con sus equivalentes, para saber mejor dónde “se hacen las cosas bien”. Además, permite la formulación de ideas que se pueden utilizar en su propio entorno. En British American Tobacco, empleábamos diversas medidas de colaboración, formales e informales, para asegurarnos de que practicábamos suficiente networking.

Nuestras relaciones más sólidas eran con los colegas del sector, seguidos de proveedores y partners, y los gobiernos en último lugar. Enviaba a los miembros del equipo a consejos asesores globales e invitaba a expertos a liderar los debates, pero también recogía información de cenas informales o discusiones durante el café. El objetivo era recopilar ideas y saber lo que las personas consideran que son las amenazas o retos emergentes. Puede parecer un poco paradójico, pero cuando la privacidad y la retención de datos se vuelve más difícil, la clave para estar más protegido es ser más abierto.

No obstante, uno debe seguir reservándose una buena dosis de cinismo sobre los grupos que deben unirse o crearse, ya que tener un número elevado de ellos diluirá el propósito y disminuirá su valor. Necesitamos dar soporte solo a los grupos más eficaces y asegurarnos de que tengan una visión de 360 grados de los riesgos potenciales.

Para que la colaboración evolucione, ciertos grupos deben estar formados exclusivamente por profesionales de la seguridad, pero otros deben estar respaldados por organizaciones de miembros, proveedores finales y partners. También deben incluirse CIOs en los grupos más amplios, no solo líderes de seguridad. Cuando se trata de colaborar, nosotros en nuestro sector podemos mirar a industrias con más experiencia para obtener ayuda. El sector financiero siempre hace todo lo posible para compartir información (particularmente información de amenazas) para proteger su gran volumen de información privada y activos financieros, creando un modelo al cual deben aspirar otros sectores industriales.

La realidad del entorno actual de amenazas en expansión es que no podemos protegerlo todo completamente. Otras compañías se enfrentan al mismo reto, por lo que conocer las perspectivas de mis compañeros ayuda a mejorar nuestras estrategias alrededor de nuestra información más sensible.

Esperar más colaboración externa

A medida que los límites de la seguridad de la información de las organizaciones se van ampliando, mezclándose y desapareciendo, los líderes de seguridad necesitarán cada vez más proteger ecosistemas enteros en lugar de limitarse a sus propias organizaciones. La protección mediante el aislamiento es cada vez menos realista en el mundo actual: el 62% de líderes de seguridad están muy de acuerdo en que el nivel de riesgo de su organización ha aumentado debido al número de interacciones y conexiones con clientes, proveedores y partners. Pero a pesar de la interconectividad generalizada que impulsa la empresa moderna, los propios líderes de seguridad no colaboran entre sí lo suficiente. Actualmente, solo el 42% de organizaciones que hemos entrevistado son miembros de un grupo de seguridad formal relacionado con el sector. No obstante, el 86% piensan que dichos grupos serán más necesarios en los próximos tres a cinco años.

Compartir la información de las amenazas

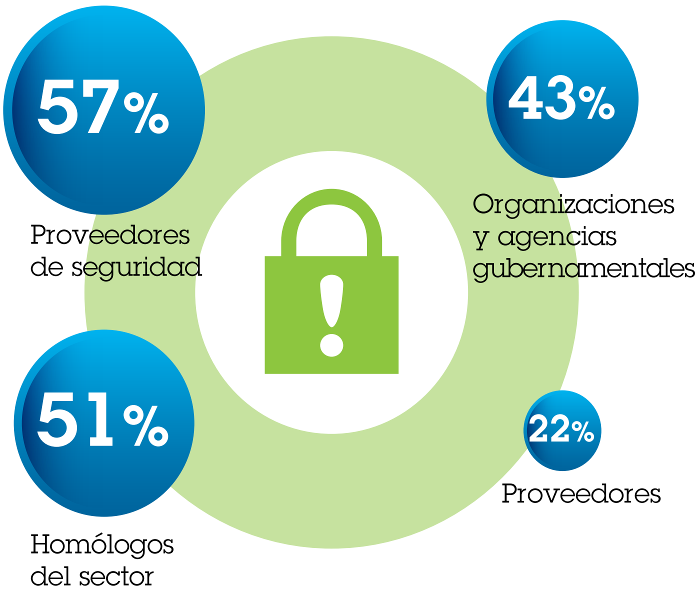


Figura 3. Para disminuir el riesgo de una conexiones más estrechas con clientes, proveedores y partners, se recomienda el enfoque “proteger el ecosistema”.

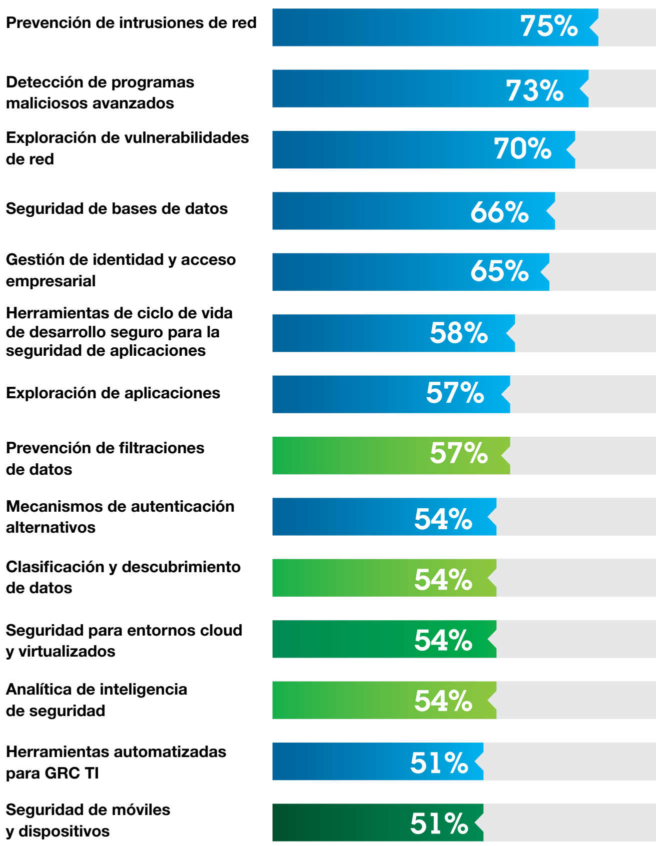
Centrándose todavía en la tecnología actual

Casi la mitad de los encuestados colocan el despliegue de nuevas tecnologías de seguridad entre sus tres iniciativas más importantes, siendo el área de máximo interés de los líderes de seguridad. Responden que son competentes en las tecnologías de seguridad establecidas, su "pan de cada día". Más del 70% se ven a sí mismos muy maduros en relación con la prevención de intrusiones en la red, detección de programas maliciosos avanzados y exploración de vulnerabilidades de red.

Sin embargo, las áreas más nuevas, tales como la prevención de filtraciones de datos, cloud y seguridad móvil, resultan ser más problemáticas: el 28% de los encuestados las identificaron como áreas necesitadas de una transformación o mejora radical, ocupando los primeros lugares de la lista de áreas necesitadas de una cierta renovación o de un enfoque distinto.

- Datos – El 72% de líderes de seguridad contestaron que la inteligencia de seguridad en tiempo real es cada vez más importante en sus organizaciones. Y aún así, áreas tales como el descubrimiento y clasificación de datos y la analítica de inteligencia de seguridad están relativamente poco maduras y con una mayor necesidad de mejora o transformación.
- Cloud – Aún existe una gran preocupación por la seguridad del cloud, pero en todo caso el consumo de cloud se ha generalizado y seguirá creciendo. El 86% de encuestados han adoptado el cloud o están planificando iniciativas de cloud. En los próximos tres a cinco años, tres cuartas partes de los líderes de seguridad esperan que su presupuesto en seguridad de cloud aumente o aumente radicalmente.
- Móvil – La mayoría de líderes de seguridad dijeron que no disponen de un enfoque de gestión de dispositivos móviles eficaz. En términos de madurez, la seguridad de móviles y terminales ocupaba la parte inferior de las tecnologías.

Madurez de la tecnología de seguridad



El 72% de líderes de seguridad contestaron que la inteligencia de seguridad en tiempo real es cada vez más importante en sus organizaciones.

En los próximos tres a cinco años, tres cuartas partes de los líderes de seguridad esperan que su presupuesto en seguridad de cloud aumente o aumente radicalmente

Menos de la mitad de líderes de seguridad nos dijeron que no disponen de un enfoque de gestión de dispositivos móviles eficaz

Figura 4. Los líderes de seguridad se ven a sí mismos muy maduros en áreas más tradicionales, mientras que la confianza no es tan alta en áreas emergentes como la analítica, el cloud o los móviles.

Poco más de la mitad de encuestados afirmaron que el mayor ritmo de la innovación en seguridad agota la capacidad de sus organizaciones para dar respuesta adecuada a las necesidades de seguridad. Presionados por desplegar, integrar y mejorar los sistemas actuales, los líderes de seguridad cuentan con poca capacidad restante para contemplar el desarrollo de tecnologías. En consecuencia, cuando se mira al futuro, más de la mitad de los encuestados no lograban imaginar otra capacidad de la seguridad que no fuese la que actualmente existe. Los líderes se concentran en la tecnología de seguridad de hoy.

Incertidumbre en la acción gubernamental

Las regulaciones, estándares y normativas son elementos con los que lidian todos los líderes de seguridad y riesgos de forma habitual. Los encuestados nos explicaron que este área seguirá siendo un factor importante de avance, aunque existe una incertidumbre substancial sobre cómo se hará exactamente.

Gran parte de la previsión de una empresa en este escenario depende de su geografía, ya que las regulaciones y estándares difieren de un país a otro y cambian constantemente. Para las empresas que operan a nivel global, tal variedad en las regulaciones crea aún más complicaciones.

Perspectiva del CISO: Resolver los retos legales y de privacidad disminuyendo la complejidad

Jamie Giroux
Vicepresidente de Seguridad y Auditoría, MAXIMUS

La complejidad de la seguridad seguirá aumentando, lo cual significa que los líderes de seguridad del futuro deberán promover la simplificación de sus procesos. Una mayor comunicación entre la vertiente tecnológica de la seguridad y la vertiente legal y de privacidad, o su completa integración, será una necesidad. No podrá proteger correctamente un sistema sin saber todo lo que conlleva: legal, privacidad, contratos, negociaciones, y la coordinación de todas estas partes diferentes.

Varios desarrollos potenciales del mercado y de la vertiente legal pueden ayudar a los líderes de seguridad del mañana. Más compatibilidad entre los productos y servicios de los proveedores permite tener una imagen panorámica de la seguridad, un único panel de instrumentos que muestre dónde existe el riesgo real en una visión de arriba a abajo. Aunque el hecho de conocer la ubicación de un ataque en la interfaz tenga valor, es más útil seguir la traza de dicho ataque hasta un servidor o escritorio. Esto es difícil si se tienen decenas de paneles de control y conjuntos de herramientas que no funcionen al unísono.

No obstante, gran parte de la oportunidad está en manos de los legisladores. Una de nuestras mayores limitaciones en Estados Unidos es que no disponemos de un estándar nacional, un mínimo común denominador en todo el país que defina un conjunto de criterios de seguridad. Cuando se trabaja para una empresa como MAXIMUS que realiza operaciones comerciales en varios sectores industriales de cada estado, todas las diferentes regulaciones suelen acabar en un conflicto.

Aunque parte del futuro de la seguridad de la información esté en nuestras manos, otra parte es conseguir una legislación adecuada. Cualesquiera requisitos comerciales y legales surjan, los líderes de seguridad deben dar forma a su tecnología para cumplirlos de la forma menos complicada posible.

Sea cual sea la ubicación, parece existir ciertas preguntas generalizadas: ¿el gobierno será un obstáculo o una ayuda? ¿Habrá más o menos colaboración y transparencia en el futuro? ¿Cómo se equilibrará la privacidad con las mayores necesidades de seguridad?

- Más de tres cuartas partes de los encuestados (79%) afirmaron que el reto planteado por las regulaciones gubernamentales y los estándares de la industria ha aumentado en los últimos tres años.
- Las regulaciones y estándares fueron una de las áreas en las que se requería un mayor esfuerzo organizativo para darles respuesta, por detrás únicamente de las amenazas externas.
- El 60% no tienen la certeza de que los gobiernos manejen la gobernanza de la seguridad a nivel nacional o global y la transparencia que tendrá.
- Solo el 22% piensan que se llegará a un acuerdo global para combatir el cibercrimen en los próximos tres a cinco años.

Fortaleciendo el futuro

¿Qué pueden hacer los líderes de seguridad para gestionar estos desafíos? ¿Cómo pueden los líderes evitar acciones que lleguen a frenar las empresas?

¿Qué pueden hacer para preparar sus organizaciones para el mañana? Encontramos cuatro acciones que los líderes de seguridad pueden llevar a cabo:

Reforzar la seguridad del cloud, los móviles y los datos

Existe un vacío de madurez entre las empresas que utilizan tecnologías de seguridad más tradicionales y las que se avanzan en áreas más nuevas. Para liberar recursos y emplearlos en áreas más nuevas, piense cuáles de sus capacidades son suficientemente maduras como para delegarlas, automatizarlas o externalizarlas.

- Las empresas están ampliamente adoptando el cloud y dedicando recursos significativos a protegerlo. El cloud puede generar dudas, pero forma parte de la empresa actual. Asegúrese de que su organización aproveche al máximo la oportunidad del cloud con el menor riesgo.
- La seguridad de los dispositivos móviles generalmente se está quedando atrás. Cuando más dispositivos estén conectados y se materialice la promesa de "Internet de las Cosas", estos problemas aumentarán. Dedique sus esfuerzos a aumentar las capacidades de seguridad de los móviles.
- No se deje abrumar por el mayor volumen de datos generados por las empresas: concéntrese en los activos más críticos. Para ayudar a gestionar la mayor amenaza externa, avance en su enfoque de la inteligencia de seguridad y analítica en tiempo real.

Mejore la formación y las habilidades de liderazgo

Preguntados por las habilidades que creen que serán necesarias en los próximos tres a cinco años, los líderes de seguridad nos respondieron que lo más importante era ofrecer cursos de formación para sus organizaciones y prepararse para adoptar un papel de mayor liderazgo. No olvide complementar el conocimiento tecnológico con las habilidades de la actividad principal, ya que están adquiriendo un papel acorde a la mayor influencia de los líderes de seguridad.

Interactúe fuera de su organización

Con la expectativa generalizada de que las conexiones con clientes, proveedores y partners aumentarán los niveles de riesgo, los líderes de seguridad deben determinar la mejor forma de proteger sus ecosistemas, no solo sus organizaciones. Realice un esfuerzo concertado para determinar la mejor forma de evaluar claramente la seguridad de cada cual: ¿cuál es la mejor forma de generar confianza entre sí y en los ecosistemas más amplios? Este requisito es especialmente crítico si se considera que solo el 14% creen que se utilizará ampliamente una forma estandarizada de evaluar y cuantificar la seguridad de la información en los próximos tres a cinco años. Utilice grupos sectoriales como canales de comunicación crítica para las buenas ideas.

Planifique varios escenarios gubernamentales

Debido a la incertidumbre sobre lo que los gobiernos pueden o no pueden hacer con respecto a la ciberseguridad, planifique varias posibilidades. Aunque cabe imaginar que los gobiernos promulgarán estándares y directrices de seguridad más alta que podrían beneficiar directamente a las empresas, no se puede confiar en dicha circunstancia.

Asegúrese de mantener un diálogo periódico con su director de privacidad (CPO) y consejo general para comprender mejor los requisitos que puedan surgir. El 72% de encuestados dicen que la privacidad del cliente es un tema de discusión cada vez más habitual con los líderes de negocio, aunque solo el 9% de líderes de seguridad colocan al CPO como uno de los tres partners más estratégicos en la empresa. Además, solo el 14% citan su consejo general como uno de sus tres partners más importantes. Adopte un enfoque completo que recabe el asesoramiento de voces externas a la función de seguridad.

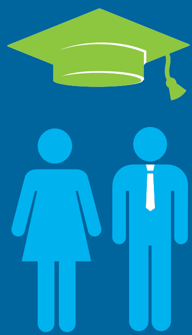
Un futuro más influyente

No cabe duda de que el avance de los peligros de la seguridad de la información resultará difícil para las personas que tengan asignada la protección de sus empresas. Pero los CISOs deben ver el futuro no como un desafío inconquistable, sino más bien como la oportunidad de elevar su nivel de aportación. La marea alta de amenazas de la última década ya ha forjado una clase superior de líderes de seguridad, capaces de capitanear su empresa a través de una persistente tormenta de grandes riesgos. Con la comprensión de los peligros para las empresas y la promulgación de intensas medidas para afrontarlos, podemos seguir proporcionando el entorno necesario para que las empresas prosperen.

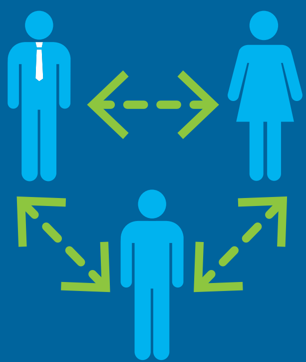
Existe una serie de acciones que los líderes de seguridad pueden realizar hoy para empezar a fortificar sus organizaciones para el futuro.



Reforzar la seguridad del cloud, los móviles y los datos
Los líderes no esperan a que las capacidades de las tecnologías futuras resuelvan sus problemas, sino que se centran en desplegar las tecnologías de seguridad actuales para minimizar sus vacíos.



Mejore la formación y las habilidades de liderazgo
Los conocimientos técnicos siguen siendo importantes, pero los conocimientos puramente comerciales cobrarán mayor importancia con la creciente influencia de los líderes de seguridad.



Participe en una mayor colaboración externa
Los líderes deben realizar un esfuerzo concertado para definir la mejor forma de generar confianza y evaluar claramente la seguridad de su ecosistema.



Planifique varios escenarios gubernamentales
El diálogo regular con directores de privacidad y consejos generales es esencial para que los líderes comprendan los requisitos que puedan surgir.

Acerca de los autores

Marc van Zadelhoff es el Vicepresidente de Estrategia Mundial y Gestión de Marketing y Producto de IBM Security Systems. Tiene más de 20 años de experiencia en estrategia, capital riesgo, desarrollo de negocio y marketing en el sector de las TI y de la seguridad. Marc trabaja con clientes en todo el mundo, asesorándoles en estrategia de seguridad y desarrollo de nuevas tecnologías para satisfacer sus necesidades. También dirige el Consejo de Asesores de Seguridad de IBM, formado por 25 CISOs importantes, que asesoran a IBM en su portfolio de seguridad. Marc fue miembro del equipo ejecutivo de la organización Consul con sede en Holanda antes de su venta a IBM en el 2007. Puede ponerse en contacto con Marc en LinkedIn y en marc.vanzadelhoff@us.ibm.com

Kristin Lovejoy es la Directora General de la División de Servicios de Seguridad de IBM, encargada del desarrollo y suministro de servicios de seguridad profesionales y gestionados a clientes de IBM de todo el mundo. Anteriormente, Kris fue Vicepresidenta de Riesgo de Tecnologías de la Información y CISO Global de IBM, responsable de la gestión, supervisión y prueba de las funciones de seguridad y resiliencia corporativas de IBM a nivel global. En la actualidad, Kris es miembro de una serie de consejos externos y paneles asesores. Es una reconocida experta en el campo de la seguridad, riesgo, cumplimiento normativo y gobierno, con apariciones en las cadenas CNBC, NPR y WTOP. Puede ponerse en contacto con Kris en LinkedIn y en klovejoy@us.ibm.com

David Jarvis es el director del equipo de investigación y de la agenda del IBM Center for Applied Insights. Está especializado en temas de tecnología y de negocio estratégicos y emergentes. Es coautor de una serie de estudios de IBM, incluidos los IBM CISO Assessments de 2012 a 2014. Además de sus responsabilidades investigadoras, David imparte cursos de previsión de negocio y resolución creativa de problemas. Puede ponerse en contacto con David en LinkedIn y en djarvis@us.ibm.com

Colaboradores

Walker Harrison
Tanya Dhamija
Yana Krasnitskaya
Ellen Cornillon
Sue Ann Wright

IBM España, S.A.
Tel.: +34-91-397-6611
Santa Hortensia, 26-28
28002 Madrid
Spain

La página de inicio de IBM se encuentra en:
ibm.com

Acerca de IBM Center for Applied Insights

ibm.com/ibmcai | **ibmcai.com**

El IBM Center for Applied Insights presenta nuevas formas de pensar, trabajar y liderar. Mediante la investigación empírica, el Centro dota a los líderes de una guía pragmática y el caso para el cambio.

WGL03061-ESES-01